PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : H04L 9/00	A2	(11) Internationale Veröffentlichungsnummer: **WO 98/39875** (43) Internationales Veröffentlichungsdatum: 11. September 1998 (11.09.98)

(21) Internationales Aktenzeichen: PCT/DE98/00677

(22) Internationales Anmeldedatum: 4. März 1998 (04.03.98)

(30) Prioritätsdaten:
197 11 037.1 4. März 1997 (04.03.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: MANNESMANN AG [DE/DE]; Mannesmannufer 2, D–40213 Düsseldorf (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: VIEWEG, Stefan [DE/DE]; Bonifatiusstrasse 53, D–40547 Düsseldorf (DE). JUNGEMANN, Matthias [DE/DE]; Lütticher Strasse 7, D–52064 Aachen (DE). SCHMIDT, Maik [DE/DE]; Lehnackerstrasse 108, D–47179 Duisburg (DE). THOENISSEN, Michael [DE/DE]; Moltkestrasse 23, D–45128 Essen (DE).

(74) Anwälte: MEISSNER, Peter, E. usw.; Hohenzollerndamm 89, D–14199 Berlin (DE).

(81) Bestimmungsstaaten: JP, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

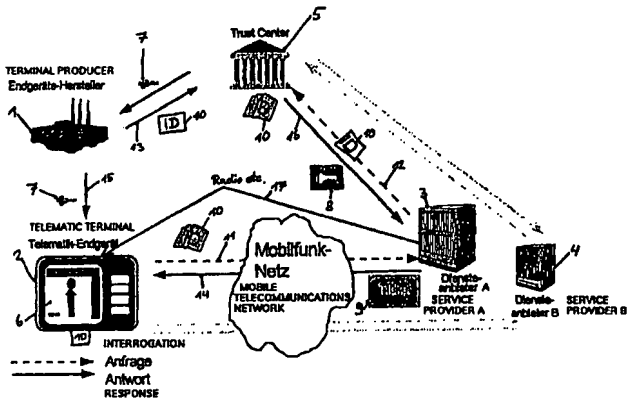
Veröffentlicht
Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.

(54) Title: METHOD FOR INSERTING A SERVICE KEY IN A TERMINAL AND DEVICES FOR IMPLEMENTING SAID METHOD

(54) Bezeichnung: VERFAHREN ZUR EINBRINGUNG EINES DIENSTESCHLÜSSELS IN EIN ENDGERÄT UND VORRICHTUNGEN ZUR DURCHFÜHRUNG DES VERFAHRENS

(57) Abstract

The invention relates to an efficient and reliable key management system comprising an inventive service center and an inventive method for introducing a service key (9) into a terminal (2). Said services key (9) can be used to enable service–key (9) encrypted data sent from a service center (3) via a communication channel to be decrypted by said terminal. The service center (3) requests (12) and obtains (16) a coding key (8) from a key center (5) when the former receives a service key transmission request (11) from a terminal (2) containing a transmitted terminal identity number (10) and which then forwards (12) said terminal identity number (10) to the key center. Said coding key (8) is allocated to a decoding key (7) inserted in the terminal (2) by the manufacturer so that service keys (9) encrypted by the coding key can be decrypted by said decoding key (7). The service center (3, 4) encrypts a service key (9) with the coding key (8) received from the key center (5) and indicates to the terminal (2) which terminal (2) can enable decryption of the service key (9) with the decoding key (7).



(57) Zusammenfassung

Eine effiziente und sichere Schlüsselverwaltung wird ermöglicht durch eine erfindungsgemäße Dienstzentrale und ein erfindungsgemäßes Verfahren zur Einbringung eines Diensteschlüssels (9) in ein Endgerät (2), durch welchen Diensteschlüssel (9) von einer Dienstzentrale (3) über einen Kommunikationskanal (14) mit einem Diensteschlüssel (9) verschlüsselt ausgesandte Dienstedaten durch das Endgerät (2) entschlüsselbar (9) sind; wobei die Dienstzentrale (3) auf eine, eine Endgeräts–Identitätsnummern Übermittlung (10) enthaltende Diensteschlüsselübermittlungsanfrage (11) des Endgeräts (2) bei der Dienstzentrale (3) hin unter Weiterübermittlung (12) der Endgeräts–Identitätsnummer (10) an eine Schlüsselzentrale (5) bei dieser (5) einen Kodierschlüssel (8) anfragt (12) und erhält (16); wobei letzterer Kodierschlüssel (8) einem dem Endgerät (2) herstellerseitig (1) eingegebenen (15) Dekodierschlüssel (7) derart zugeordnet ist, daß mit dem Kodierschlüssel (8) verschlüsselte Diensteschlüssel (9) mit dem Dekodierschlüssel (7) entschlüsselbar sind; wobei die Dienstzentrale (3, 4) mit dem von der Schlüsselzentrale (5) erhaltenen Kodierschlüssel (8) einen Diensteschlüssel (9) verschlüsselt und dem Endgerät (2) übermittelt, in welchem Endgerät (2) der Diensteschlüssel (9) mit dem Dekodierschlüssel (7) entschlüsselbar ist.

Verfahren zur Einbringung eines Diensteschlüssels in ein Endgerät und Vorrichtungen zur Durchführung des Verfahrens

Beschreibung

Die Erfindung betrifft ein Verfahren zur Einbringung eines Diensteschlüssels in ein Endgerät und Vorrichtungen zur Durchführung des Verfahrens.

Von einer Verkehrstelematikdienst-Zentrale werden über einen privaten (z.B. Mobilfunk) oder öffentlichen (z.B. DAB-Radio, RDS-TMC-Radio) Kommunikationskanal Dienstedaten an mindestens ein Endgerät übersandt. Dienstedaten können beispielsweise Daten für Verkehrsinformationen, Verkehrsprognosen, Navigationsdienste usw. sein, die von der Zentrale unidirektional an das Endgerät gesendet werden oder im bidirektionalen Dialog zwischen der Zentrale und dem Endgerät auf Anfrage übermittelt werden. Da die Erfassung und Aufbereitung derartiger Daten mit Kosten verbunden ist, werden sie in der Regel nur an zahlende Subscriber (gebuchte Dienstnutzer) übermittelt. Hierfür werden Dienstedaten von der Zentrale verschlüsselt an das Endgerät übermittelt. Dazu müssen im Endgerät und in der Zentrale zueinander passende Schlüssel vorgesehen sein. Bei bestimmten Anwendungen kann es auch wünschenswert sein, Diensteschlüssel für nur für einen Zeitraum gebuchte Dienstedaten im Endgerät nach einiger Zeit verfallen zu lassen oder zu aktualisieren. Hinsichtlich der Schlüsseleinbringung ist deshalb ein relativ hohes Sicherheitsniveau zur Vermeidung von Mißbrauch erforderlich. Bekannt aus anderen Bereichen, wie Fernsehen (Pay-TV), sind Verschlüsselungs- und Authentifizierungs-Verfahren. Zur Verschlüsselung und Entschlüsselung sind grundsätzlich symmetrische Verfahren (mit gleichem Verschlüsselungsschlüssel wie Entschlüsselungsschlüssel) und asymmetrische Verfahren (mit zueinander passendem, aber unterschiedlichem Verschlüsselungsschlüssel und Entschlüsselungsschlüssel) bekannt.

Aufgabe der Erfindung ist eine möglichst einfache, effiziente, kostengünstige Optimierung schlüsselbezogener Vorgänge. Die Aufgabe wird durch die Gegenstände der unabhängigen Ansprüche gelöst.

Die Erfindung ermöglicht eine einfache, effiziente und sichere Schlüsseleinbringung. Auch die Einbringung neuer Diensteschlüssel, welche beispielsweise nach Ablauf eines Subscriptions-Zeitraums für einen bestimmten Dienst erforderlich sein kann, wird einfach, effizient und sehr sicher ermöglicht. Dabei ist es zur Einbringung eines neuen Diensteschlüssels nicht erforderlich, das Endgerät in eine Werkstätte des Endgerät-Herstellers oder Dienste-Anbieters zu bringen; die Einbringung eines neuen Diensteschlüssels ist vielmehr erfindungsgemäß über Kommunikationskanäle, insbesondere Telefonfestnetz oder Mobilfunk, insbesondere Mobilfunk-Kurznachricht, möglich. Auch die Kommunikation zwischen einem Endgerät-Hersteller und einer Schlüsselzentrale (= Trust-Center) und/oder zwischen einer Dienstzentrale (Dienste-Anbieter) und einer Schlüsselzentrale und/oder zwischen Geräten eines Endgeräte-Herstellers und (bei der Entschlüsselungs-Schlüsseleinbringung bei der Herstellung) einem Telematik-Endgerät kann über einen Kommunikationskanal, wie insbesondere Mobilfunk (z.B. Mobilfunk-Kurznachrichten) erfolgen.

Für ein sicheres und dabei effizient ausführbares Verfahren ist es vorteilhaft, daß die Schlüssel-Behandlung in mehrere Phasen unterteilt ist. Dabei entspricht die erste Phase der Ausstattung eines Endgerätes mit einem herstellerspezifischen Schlüssel (Dekodierschlüssel). Die zweite Phase beinhaltet die verschlüsselte, insbesondere asymmetrisch verschlüsselte, Einbringung eines Diensteschlüssels von der Dienstzentrale zum Endgerät unter Verwendung eines Kodierschlüssels in der Dienstzentrale und eines Dekodierschlüssels im Endgerät. Die dritte Phase beinhaltet insbesondere die Verschlüsselung von Dienstedaten im Rahmen eines Dienstes und deren Übermittlung zwischen der Dienstzentrale und dem Endgerät; dabei werden im unidirektionalen Betrieb von der Dienstzentrale Dienstedaten verschlüsselt an das Endgerät gesandt und dort mit dem Diensteschlüssel entschlüsselt, während im bidirektionalen Verfahren eine Verschlüsselung von Anfragen eines Endgerätes bei der Dienstzentrale und/oder von übertragenen Dienstedaten der Dienstzentrale an das Endgerät möglich ist. Die Verschlüsselung von Dienstedaten mit einem symmetrischen Schlüssel ist besonders vorteilhaft, weil damit in Echtzeit relativ große Datenmengen im Rahmen eines Dienstes verschlüsselt und endgerätseitig ohne

übermäßigen Aufwand in Echtzeit entschlüsselt werden können. Die asymmetrische Verschlüsselung des Diensteschlüssels ergibt hingegen die für seine Übertragung erforderliche höhere Sicherheit.

Besonders vorteilhaft ist die zusätzliche Nutzung von netzseitigen Sicherheitsmechanismen bei der Einbringung eines Diensteschlüssels von einer Dienstzentrale in das Endgerät, und zwar bei der Kommunikation zwischen der Dienstzentrale und der Schlüsselzentrale und/oder zwischen der Dienstzentrale und dem Endgerät. Ferner können netzseitige Sicherheitsmechanismen insbesondere auch verwendet werden, wenn der Endgeräte-Hersteller einen Entschlüsselungsschlüssel bei der Herstellung über ein Mobilfunknetz etc. in ein Telematik-Endgerät einbringt; jedoch ist bei der Herstellung auch eine Einbringung eines Entschlüsselungsschlüssels im Endgerät ohne einen Mobilfunkkanal etc. durch Hardware-Installation oder Software-Installation möglich. Netzseitige Sicherheitsmechanismen können bei der Kommunikation über ein Mobilfunknetz insbesondere SMSC-Adressen, MSISDN PIN-Nummer, PIN2-Nummer, etc. im GSM-Netz oder in anderen Netzen standardisiert vorgesehene Authentifikationsprüfungen sein. Die netzseitigen Sicherheitsmechanismen werden dabei zusätzlich zu anderen, insbesondere erfindungsgemäßen Mechanismen verwendet.

Die Endgerät-Identitätsnummer kann eine beliebige Nummer sein, welche ein bestimmtes Endgerät identifiziert. Sie kann im Endgerät insbesondere bei der Herstellung als Hardware und/oder Software fest eingegeben sein. Zweckmäßig ist sie gegen Manipulation und/oder unberechtigtes Auslesen geschützt.

Erfindungsgemäß kann ein Endgerät auch Diensteschlüssel von mehreren Dienstzentralen bekommen und zur Entschlüsselung von jeweils deren Dienstedaten verwenden.

Das erfindungsgemäße Verfahren ist dienstzentralen- seitig insbesondere als Programm realisierbar. Erfindungswesentliche Merkmale, wie das Verwalten von Dekodierschlüsseln und Diensteschlüsseln sind im Endgerät vorgesehen; die Behandlung von zueinander passenden Kodierschlüsseln und Dekodierschlüsseln sowie eventuell zusätzlich der Endgeräts-Identitätsnummer sind in einer Schlüsselzentrale realisiert.

Weitere wesentliche Merkmale der Erfindung sind in den Unteransprüchen sowie in der nachfolgenden Beschreibung eines Ausführungsbeispiels anhand der Zeichnung beschrieben. Dabei zeigt

Fig. 1 schematisch grob abstrahiert die erfindungsgemäße Verwendung von Diensteschlüsseln, Kodierschlüsseln und Dekodierschlüsseln,

Fig.2 eine Abwandlung der Version in Figur 1.

Figur 1 zeigt einen Endgerät-Hersteller 1, ein Endgerät 2 für Verkehrstelematikdienste, zwei Dienstzentralen 3,4, sowie eine Schlüsselzentrale 5.

Ein Endgerät 2 für Verkehrstelematikdienste kann beispielsweise zum Darstellen von Verkehrsinformationen und/oder Verkehrsprognosen und/oder Navigationsinformationen ausgebildet sein. Dabei können am Verkehrstelematikendgerät für interaktive Dienste wie Navigationshilfen interne oder externe Eingabemittel wie Tastaturen, Spracheingabe etc. vorgesehen sein. Ferner kann im Endgerät 2 eine Aufbereitung von Dienstedaten und/oder Positionserfassung etc. erfolgen. Die Ausgabe kann optisch und/oder akustisch erfolgen. Im dargestellten Beispiel wird in einem Display 6 im Endgerät 2 die Position des Endgerätes mit einem Pfeil und einem Punkt gekennzeichnet, sowie eine nahegelegene Straße mit Name und Entfernungsangabe angeben, sowie darüber eine weitere Straße als Balken angegeben. Jedoch ist das erfindungsgemäße Verfahren auch für beliebige anders aufgebaute Endgeräte einsetzbar.

Bei der Herstellung des Endgerätes 2 beim Endgerätehersteller 1 wird vom Endgerätehersteller in das Endgerät 2 ein als Symbol dargestellter Dekodierschlüssel 7 eingebracht, welcher (bei einem insbesondere asymmetrischen Verfahren) zur Dekodierung eines in einer Dienstzentrale mit einem (ebenfalls symbolisch dargestellten) Kodierschlüssel 8 verschlüsselten Diensteschlüssels 9 verwendbar ist. Hier wird mit dem Kodierschlüssel 8 verschlüsselt ein Diensteschlüssel 9 (in Figur 1 bezeichnet als " Ticket") von einer Dienstzentrale 3 oder 4 an ein Endgerät 2 übertragen, wodurch dem Endgerät mit dem Diensteschlüssel 9 die Dekodierung von Dienstedaten (betreffend Verkehrsinformation, Navigation etc.) ermöglicht wird, welche eine Dienstzentrale 3, 4 zu einem beliebigen Zeitpunkt (mit einem derartigen

Diensteschlüssel 9 verschlüsselt) über einen öffentlichen Kommunikationskanal wie Radio (DAB, RDS-TMC etc.) aussendet (17).

Bei der Herstellung des Endgerätes 2 beim Endgerätehersteller 1 wird in das Endgerät 2 neben dem Dekodierschlüssel 7 auch eine Endgerät- Identifikationsnummer fest implementiert. Die Endgeräts-Identifikationssnummer kann jedoch bereits vor der Fertigstellung (mit Dekodierschlüsseleingabe) des Endgeräts beim angegebenen Endgerätehersteller im Endgerät (zu einem früheren Zeitpunkt bei einem Zulieferer etc.) implementiert sein. Die Endgeräts- Identitäts- Nummer muß nicht nur aus Zahlen bestehen, sondern kann beispielsweise auch Buchstaben umfassen. Sie kann eine beliebige, ein Endgerät identifizierende, im Endgerät implementierte Sequenz sein.

Der Dekodierschlüssel 7, welcher von dem Endgerätehersteller 1 dem Endgerät 2 bei der Herstellung (oder analog bei einer späteren Anpassung des Endgerätes an das erfindungsgemäße Schlüssel- System) implementiert wird, wird dem Endgerätehersteller 1 von einer Schlüsselzentrale 5 übermittelt. Die Übermittlung von der Schlüsselzentrale zum Endgerätehersteller kann dabei auch kodiert oder mit sonstigen Sicherheitsmaßnahmen erfolgen. Ferner wird im Beispiel in Figur 1 vom Endgerätehersteller 1 an die Schlüsselzentrale 5 eine Endgeräts-Identitätsnummer übertragen, welche der Schlüsselzentrale die Zuordnung des Dekodierschlüssels 7 zu einer Endgeräts- Identitätsnummer und damit zu einem Endgerät erlaubt. Damit kann bei einer Anfrage der Dienstzentrale 3 oder 4 (auf eine Anfrage des Endgeräts 2 mit der Endgeräts-Identitätsnummer 10 bei der Dienstzentrale 3 oder 4 mit der Bitte um einen Diensteschlüssel 9 hin) mit Angabe der (weitergegebenen) Endgeräts- Identitätsnummer 10 die Schlüsselzentrale 5 über die Endgeräts- Identitätsnummer 10 dem schon vergebenen (hier auf ein bestimmtes Endgerät 2 bezogenen) Dekodierschlüssel 7 den passenden Kodierschlüssel 8
(welcher letzterer von der Schlüsselzentrale an die Dienstzentrale 4 übergeben werden soll) zuordnen. Die Zuordnung kann jedoch auch aufgrund Daten innerhalb des Kodierschlüssels und Dekodierschlüssels erfolgen; beispielsweise können in diesem Fall bestimmte Bit- Sequenzen im Kodierschlüssel oder Dekodierschlüssel übereinstimmen oder in der Dienstzentrale bekannt oder einander zugeordnet sein.

Der Ablauf zum kodierten Einbringen eines Diensteschlüssels 9 (für Dienstedaten) von einer Dienstzentrale 3 oder 4 in ein Endgerät 2 kann insbesondere folgendes umfassen:

Das Endgerät 2 fragt (im Schritt 11) bei einer Dienstzentrale 3 oder 4 nach einem Diensteschlüssel. Dabei übergibt das Endgerät 2 seine Endgeräts- Identitätsnummer etc. an die Dienstzentrale 3 oder 4. Diese Kommunikation kann über ein Kommunikationsnetz, insbesondere Mobilfunknetz, z. B. als Mobilfunk-Kurznachricht (zum Beispiel GSM-SMS) erfolgen ebenso wie die darauf folgende Antwort. Die Dienstzentrale überprüft, ob sie für das (durch die übermittelte Endgeräts-Identitätsnummer 10 etc. identifizierte) Endgerät 2 einen Kodierschlüssel 8 (zum kodieren von zu übermittelten Diensteschlüsseln) hat. Im vorliegenden Fall hat die Dienstzentrale 3, 4 noch keinen Kodierschlüssel 8 für das Endgerät 2. Sie fragt deshalb im Schritt 12 unter Übermittlung der (vom Endgerät übermittelten) Endgeräts-Identitätsnummer bei der Schlüsselzentrale um Übermittlung eines Kodierschlüssels 8 an. Dabei kann die Kommunikation zwischen der Dienstzentrale und der Schlüsselzentrale über einen Kommunikationskanal wie z. B. Mobilfunk, insbesondere Mobilfunk-Kurznachricht (insbesondere GSM-SMS) erfolgen. Die Schlüsselzentrale 5 überprüft hier anhand der von der Dienstzentrale 3, 4 an sie übermittelten Endgeräts-Identitätsnummer 10, ob sie einen zur Endgeräts- Identitätsnummer passenden Kodierschlüssel 8 für das Endgerät 2 hat. Wenn ein Kodierschlüssel 8 der Endgeräts-Identitätsnummer 10 etc. zuordenbar ist, übermittelt die Schlüsselzentrale 5 der Dienstzentrale 3 oder 4 einen zum Endgerät 2 passenden Kodierschlüssel 8. Die Dienstzentrale 4 kodiert mit dem Kodierschlüssel 8 einen Diensteschlüssel und übermittelt ihn (im Schritt 14) an das Endgerät 2. Das Endgerät 2 dekodiert mit seinem (bei der Herstellung etc. implementierten) Dekodierschlüssel 7 den (kodiert übermittelten) Diensteschlüssel 9. Darauf kann das Telematikendgerät 2 auf diesen Diensteschlüssel 9 bezogene Daten, welche einer Dienstzentrale 3 oder 4 per Mobilfunk oder per Radio etc. (mit 9 verschlüsselt) ausstrahlt mit dem Diensteschlüssel 9 dekodieren. Für verschiedene Dienste einer Dienstzentrale können jeweils eigene Diensteschlüssel 9 vorgesehen sein.

Die Ermöglichung der Zuordnung einer von der Dienstzentrale an die Schlüsselzentrale 5 übermittelten Endgeräts-Identitätsnummer 10 zu einem zugehörigen Kodierschlüssel 8 erfolgt im Beispiel in Figur 1 folgendermaßen: Bei der Herstellung des Endgeräts 2 beim Endgerätehersteller 1 fragt der Endgerätehersteller

unter Übergabe der Endgeräts- Identitätsnummer 10 bei der Schlüsselzentrale 5 um Übermittlung eines Dekodierschlüssels 7 an. Die Schlüsselzentrale 5 ordnet intern die (im Schritt 13 übermittelte) Endgeräts-Identitätsnummer 10 des Endgerätes 2 demjenigen Dekodierschlüssel 7 zu, welchen sie für das Endgerät 2 mit der speziellen übermittelten Endgeräts-Identiätsnummer 10 dem Endgerätehersteller 1 (zur Weitergabe an das Endgerät 2 im Schritt 15) übermittelt. Dabei ordnet die Schlüsselzentrale 5 der Endgeräts-Identitätsnummer 10 eines bestimmten Endgerätes 2 einen zu dem (dem Endgerät übermittelten) Dekodierschlüssel 7 passenden Kodierschlüssel 8 zu, welcher später einer Dienstzentrale 3 oder 4 übermittelt wird, wenn sie unter Angabe der Endgeräts-Identitätsnummer 10 (im Schritt 12) bei der Schlüsselzentrale um einen Kodierschlüssels anfragt. Damit ist gewährleistet, daß die Dienstzentrale 3 oder 4 einen Kodierschlüssel 8 kennt, der zu einem Dekodierschlüssel 7 paßt, welcher in einem Endgerät 2 implementiert ist, und daß die Dienstzentrale 3 oder 4 den Kodierschlüssel 8 aufgrund der Endgeräts-Identitätsnummer 10 zuordnen kann, so daß eine Dienstzentrale 3 oder 4 über den Kodierschlüssel 8 an ein hier bekanntes Endgerät 2 gezielt einen (nur von diesem mit seinem Dekodierschlüssel 7 entschlüsselbaren) Diensteschlüssel 9 für einen bestimmten Dienst übermitteln kann.

Jedoch sind (wie in Figur 2 angedeutet) auch andere Zuordnungsmöglichkeiten des Kodierschlüssels und Dekodierschlüssels in der Schlüsselzentrale 5 möglich; Diese können insbesondere in einer Zuordnung von Anfangssequenzen (oder analog Schlußsequenzen) in einem Dekodierschlüssel 7 bestehen, welche Anfangssequenzen im Kodierschlüssel 8 identisch sind oder (in der Schlüsselzentrale 5 und/oder einer Dienstzentrale 3, 4 bekannte Weise) entsprechen. Derartigen Anfangssequenzen in einem Kodierschlüssel und Dekodierschlüssel sind einer Endgeräts- Identitätsnummer 10 gemäß dem Beispiel in Figur 1 äquivalent. Beispielsweise kann eine Schlüsselzentrale 5 einem Endgerätehersteller in einem Datensatz mit dem eigentlichen Dekodierschlüssel 7 zusammen eine Anfangssequenz etc. übermittelten, die dort (1) in das Endgerät eingegeben wird; bei einer Diensteschlüsselanfrage 11 des Endgerät bei einer Dienstzentrale kann das Endgerät diese Anfangssequenz etc. an die Dienstzentrale 3 übergeben, welche diese an die Schlüsselzentrale weiterübergibt (12), wo eine Zuordnung zu einem (zum Dekodierschlüssel des Endgeräts passenden) Kodierschlüssel erfolgt, welcher letzterer (8) der Dienstzentrale 3 übergeben (3) wird.

Patentansprüche

1. Verfahren zur Einbringung eines Diensteschlüssels (9) in ein Endgerät (2), durch welchen Diensteschlüssel (9) von einer Dienstzentrale (3) über einen Kommunikationskanal (14) mit einem Diensteschlüssel (9) verschlüsselt ausgesandte Dienstedaten durch das Endgerät (2) entschlüsselbar (9) sind,

wobei die Dienstzentrale (3) auf eine, eine Endgeräts-Identitätsnummern-Übermittlung (10) enthaltende Diensteschlüsselübermittlungsanfrage (11) des Endgeräts (2) bei der Dienstzentrale (3) hin unter Weiterübermittlung (12) der Endgeräts-Identitätsnummer (10) an eine Schlüsselzentrale (5) bei dieser (5) einen Kodierschlüssel (8) anfragt (12) und erhält (16),

wobei letzterer Kodierschlüssel (8) einem dem Endgerät (2) herstellerseitig (1) eingegebenen (15) Dekodierschlüssel (7) derart zugeordnet ist, daß mit dem Kodierschlüssel (8) verschlüsselte Diensteschlüssel (9) mit dem Dekodierschlüssel (7) entschlüsselbar sind,

wobei die Dienstzentrale (3), (4) mit dem von der Schlüsselzentrale (5) erhaltenen Kodierschlüssel (8) einen Diensteschlüssel (9) verschlüsselt und dem Endgerät (2) übermittelt, in welchem Endgerät (2) der Diensteschlüssel (9) mit dem Dekodierschlüssel (7) entschlüsselbar ist.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
daß eine Dienstzentrale (3) von einer Schlüsselzentrale (5) einen Kodierschlüssel (8) nur im Falle einer der Schlüsselzentrale (5) bekannten Endgeräts-Identitätsnummer (10) erhält.

3. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Endgeräts-Identitätsnummer (10) der Schlüsselzentrale (5) vom Endgerätehersteller übermittelt wird, wenn dieser (1) bei der Schlüsselzentrale (5) einen Dekodierschlüssel (7) anfragt, wobei in der Schlüsselzentrale (5) die Endgeräts-Identitätsnummer (10) dem übergebenden Dekodierschlüssel (7) und einem einer Dienstzentrale (3) auf Anfrage zu übergebenden Kodierschlüssel (8) zu geordnet wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Dienstzentrale eine Verkehrstelematik - Dienstzentrale ist, daß der Diensteschlüssel ein Diensteschlüssel zum Entschlüsseln von Verkehrstelematikdienst- Daten ist und daß das Endgerät für Verkehrstelematikdienste verwendbar ist.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Übermittlung zwischen dem Endgerät und der Dienstzentrale per Funk, insbesondere Mobilfunk, insbesondere Point to Point - Mobilfunkkurznachricht (GSM-SMS) erfolgt.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Kommunikation zwischen der Dienstzentrale (3) und der Schlüsselzentrale (5) über ein Telefonfestnetz oder per Funk, insbesondere Mobilfunk, insbesondere Point-to-Point - Mobilfunk Kurznachricht (GSM - SMS) erfolgt.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß bei einer Kommunikation auf Mobilfunk - spezifische Sicherheitsfunktionen, insbesondere Telefonnummer und/oder MSISDN und/oder PIN-Nummer, zurückgegriffen wird, wobei eine Schlüsselübermittlung nur bei erfolgreicher Sicherheitsüberprüfung erfolgt.

8. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
daß ein Endgerät (2) von mehreren Dienstzentralen (3), (4) Diensteschlüssel (9) und/oder über eine Schlüsselzentrale (5) zugehörige Dekodierschlüssel (7) erhalten kann.

9. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
daß Diensteschlüssel von einer Dienstzentrale (3) an ein Endgerät (2) asymmetrisch verschlüsselt übertragen werden.

10. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
daß Dienstedaten von einer Dienstzentrale an ein Endgerät (2) symmetrisch verschlüsselt übertragen (17) werden.

11. Dienstzentrale zur Durchführung des Verfahrens nach einem der vorhergehenden Ansprüche.

12. Dienstzentrale nach Anspruch 11,
dadurch gekennzeichnet,
daß sie ein Programm zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 10 aufweist.

13. Dienstzentrale nach einem der Ansprüche 11 bis 12,
dadurch gekennzeichnet;
daß sie folgendes aufweist:
- eine Mobilfunkkommunikationseinrichtung zum Übertragen eines verschlüsselten Diensteschlüssel an ein Endgerät (2),
- eine Kommunikationseinrichtung zum Kommunizieren mit einer Schlüsselzentrale,
- eine Einrichtung zum Verschlüsseln eines Diensteschlüssels mit einem Kodierschlüssel,
- einen Speicher für Kodierschlüssel und Diensteschlüssel.

14. Dienstzentrale nach einem der Ansprüche 11 bis 13,
dadurch gekennzeichnet,
daß sie eine symmetrische Verschlüsselungseinrichtung für Dienstedaten aufweist.

15. Dienstzentrale nach einem der Ansprüche 11 bis 13,
dadurch gekennzeichnet
daß sie eine asymmetrische Verschlüsselungseinrichtung für Diensteschlüssel oder/ und Dienstedaten aufweist.

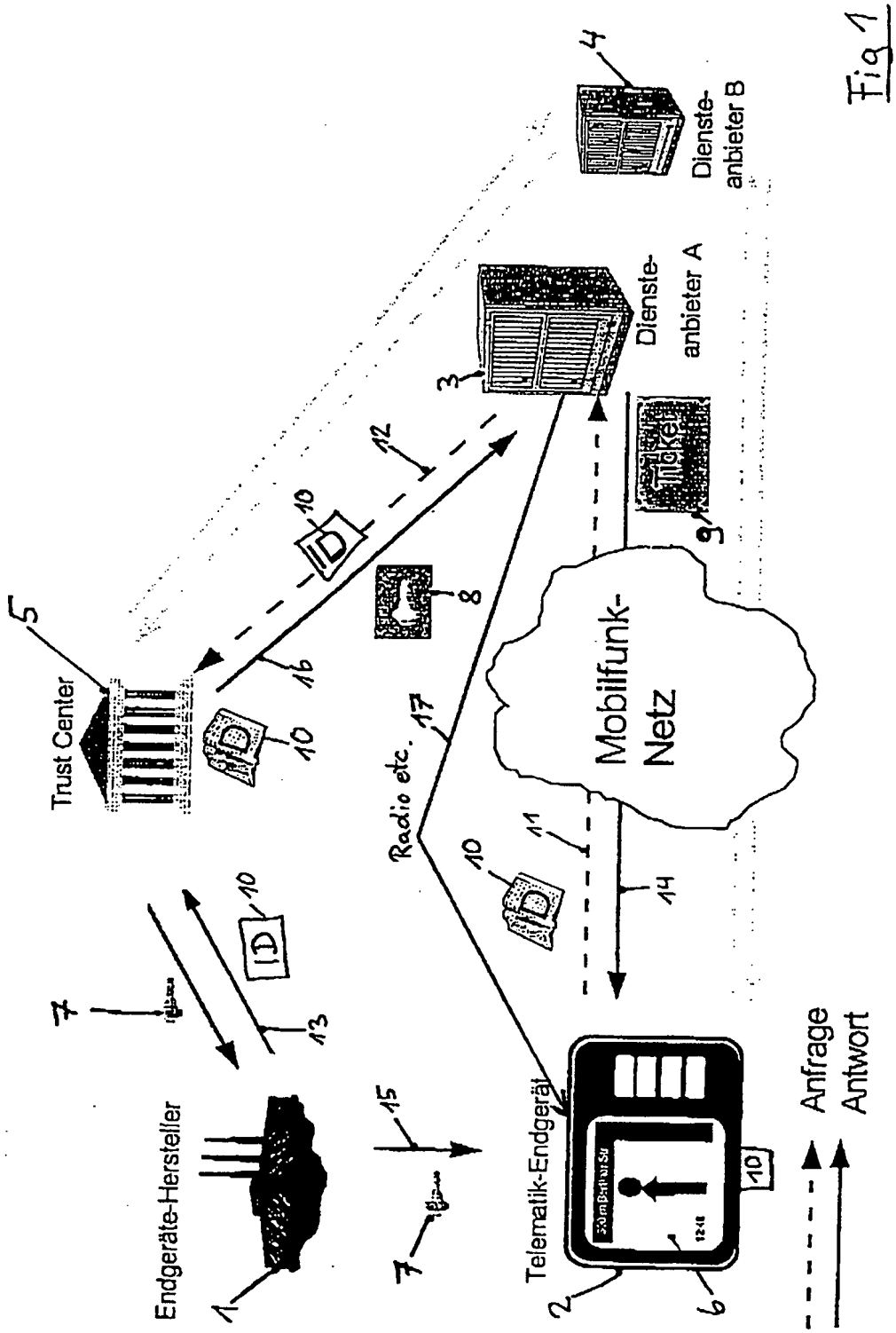

Trust Center
Endgeräte-Hersteller
Telematik-Endgerät
Mobilfunk-Netz
Dienste-anbieter A
Dienste-anbieter B
Radio etc.
Anfrage
Antwort
ID
Ticket

Fig 1

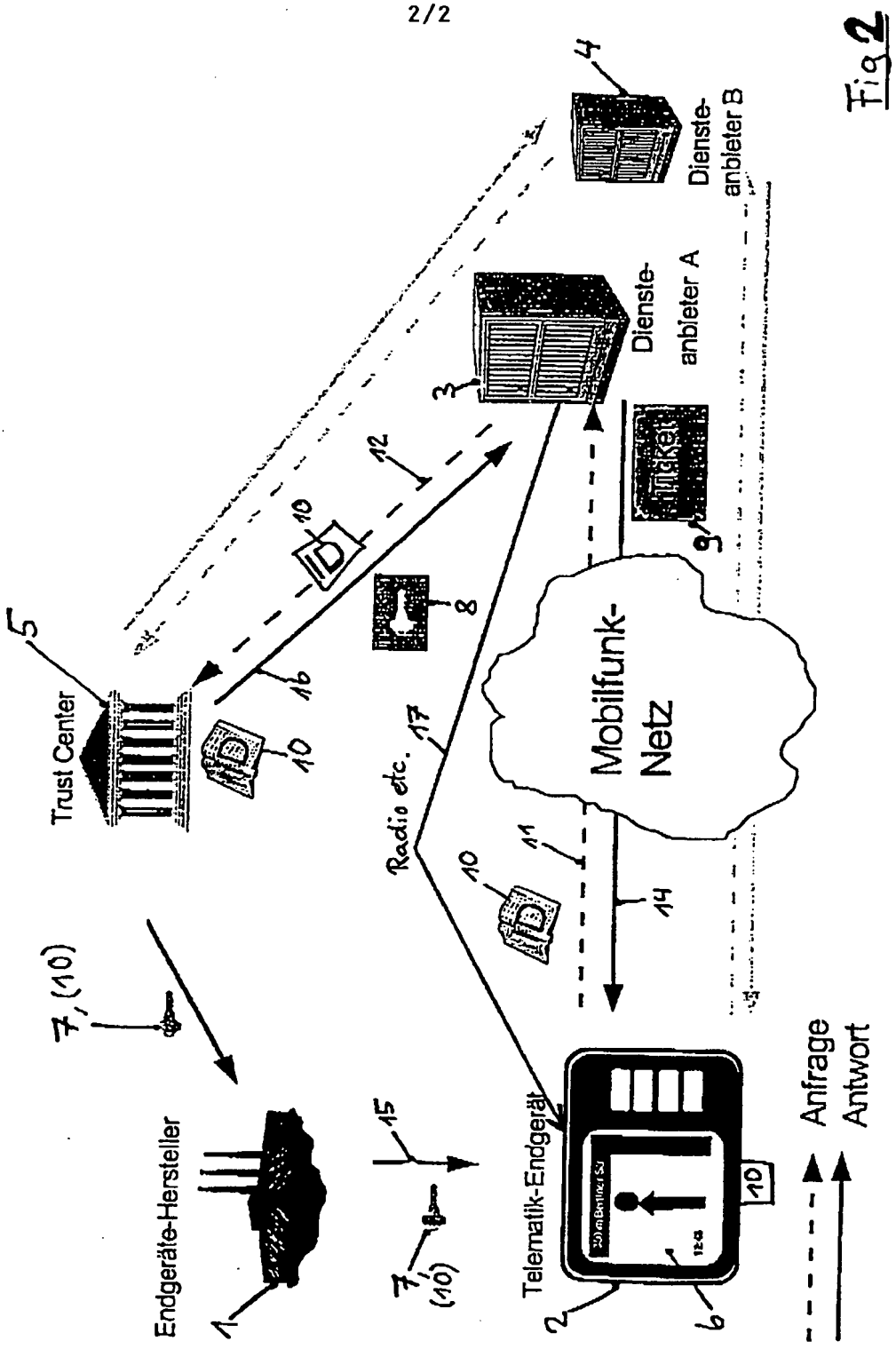

Trust Center
Radio etc.
Mobilfunk-Netz
Dienste-anbieter A
Dienste-anbieter B
Endgeräte-Hersteller
Telematik-Endgerät
Anfrage
Antwort

Fig 2